The Future of Transatlantic Data Flows

Consumers, Businesses, and Economic Growth Depend on Transatlantic Data Flows.

Companies of all sizes and in all industries need to move data across the Atlantic to reach customers, manage supply chains, collaborate on research, and improve the services they provide to businesses and individuals. And customers—on both sides of the Atlantic—deserve to know that their personal data will be maintained private and secure when their data is transferred. Transatlantic data flows are among the most important for both Europe and the US, accounting for over one-half of Europe's data transfers and about half of US data transfers.[1] A disruption of transatlantic data flows could have significant adverse effects on consumers, businesses, and economic vitality.

How Personal Data Is Transferred From the EU.

European Union law generally prohibits companies from transferring personal data from the EU to another country unless companies use an approved transfer mechanism. The approved transfer mechanisms are designed to ensure that EU fundamental rights are protected regardless of where the personal data is transferred. Currently, personal data can be transferred from the EU to another country through a determination by the European Commission that the other country's privacy protections are "adequate," or through Commission-approved commitments such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs).

The *Schrems II* Ruling Limited Organizations' Ability to Transfer Data.

The European Court of Justice (ECJ) recently considered the validity of the EU-US Privacy Shield Framework ("Privacy Shield") and the use of SCCs to transfer data outside the EU. BSA participated as an amicus in the case, arguing that SCCs were intended to be used for transfers to countries that did not have an adequacy decision, and that a case-by-case decision must be made on whether their use provides sufficient protection.

On July 16, 2020, the ECJ invalidated the Privacy Shield as a mechanism for transferring data across the Atlantic in *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ("*Schrems II*"). It ruled, however, that SCCs remain a valid data transfer mechanism between the EU and US, though entities using SCCs (the exporter and the importer) are required to verify, on a case-by-case basis, whether the personal data can be provided the required privacy protection in the country where the data is transferred.

[1] Hamilton, Daniel S. and Joseph P. Quinlan, The Transatlantic Economy 2020: Annual Survey of Jobs, Trade and Investment between the United States and Europe (Mar. 26, 2020), available at: https://transatlanticrelations.org/wp-content/uploads/2020/03/TE2020_Report_FINAL.pdf.

What Is the Privacy Shield? Why Is It Important?

The Privacy Shield was an important tool for transferring data between the US and EU. The Privacy Shield was a voluntary program, negotiated by the US Government and European Commission, that allowed companies to self-certify to a set of privacy principles that ensure data is "adequately" protected when transferred to the US.[2] Over 5,200 organizations across a range of industries relied on the Privacy Shield to transfer data, more than 70% of which were small- or medium-sized businesses. BSA supports continued efforts by the European Commission and US Government to build on the Privacy Shield and ensure a similar mechanism can be used for EU-US transfers in the future.

What Are SCCs? Why Are They Important?

SCCs are a vital, privacy protective mechanism used by millions of companies—European, American, and others—that transfer data in and out of Europe. SCCs impose a range of contract-based obligations on exporters and importers of personal data. These obligations—which are legally binding and fully enforceable under EU law—ensure that protections under the EU's General Data Protection Regulation (GDPR) apply to personal data transferred in accordance with these agreements. Today, SCCs underpin transfers of personal data from the EU not only to the US, but to over 180 countries—including Australia, Singapore, South Korea, Brazil, India, and Mexico, among many others. Without SCCs, companies around the world—both in and out of the EU—would have to curtail services significantly and customers would suffer as a result.

According to a 2019 IAPP-EY report, approximately 88% of companies transferring data out of the EU rely on SCCs, while 60% used Privacy Shield.[3]

Consumers and Businesses Need a Reliable, Long-Term Mechanism for Transatlantic Data Transfers.

US and EU policymakers should work together to support efforts that sustain reliable mechanisms for transatlantic data transfers, which would ensure consumers have access to goods and services, businesses understand their obligations, and innovation and economic growth are uninhibited. Specifically, policymakers should advocate SCCs as a trusted, responsible tool to transfer data outside of Europe. Policymakers should also encourage the development of an enhanced successor framework to the Privacy Shield that establishes strong privacy protections, provides clear guidelines for businesses, and fosters trust on both sides of the Atlantic.

[2] The Privacy Shield was a partial adequacy decision for companies under the authority of the US Federal Trade Commission.

[3] IAPP-EY Annual Governance Report 2019 (Nov. 6, 2019), available at: https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/.